JENS SYCKOR / THORSTEN STRUFE / ANNE LAUBER-RÖNSBERG

Die Datenschutz-Folgenabschätzung: Ausnahme oder Regelfall?

Wann muss eine Datenschutz-Folgenabschätzung durchgeführt werden?

Pflichten des Verantwortlichen
Schwellwertanalyse
Praxisnahe Vorprüfung
Risikobasierter Ansatz

■ Die Datenschutz-Folgenabschätzung, eine wesentliche Ausprägung des risikobasierten Ansatzes der DS-GVO, ist durchzuführen, wenn eine Form der Verarbeitung mit einem hohen Risiko für die Betroffenen einhergeht. Der Beitrag untersucht, wie der Schwellwert des „hohen Risikos" und die in Art. 35 Abs. 1 DS-GVO genannten Indikatoren präzisiert werden können, um die Vorprüfung, ob eine Datenschutz-Folgenabschätzung durchzuführen ist, in der Praxis zu erleichtern. Hierbei wird dafür plädiert, i.R.d. Vorprüfung lediglich die Eingriffsintensität, hingegen nicht die Eintrittswahrscheinlichkeit des Schadens einzubeziehen. Die entwickelten Grundsätze werden sodann auf zwei Beispiele angewendet, die aufzeigen, welche Unsicherheiten dennoch bei der Vorprüfung in der Praxis entstehen können.
Lesedauer: 25 Minuten

■ The assessment of consequences of data protection, a substantial manifestation of the risk-based approach of the General Data Protection Regulation (GDPR/DS-GVO) shall be implemented if a form of processing is accompanied by a high risk for the affected person. This article will investigate how the threshold of „high risk" and the indicators listed in Art. 35 Subsec. 1 GDPR can be made more precise in order to make the pre-review easier in practice whether an assessment of consequences of data protection shall be conducted. In this it is argued to only include the intensity of the interference in the scope of the pre-review rather than the likelihood of the occurrence of damages. The developed principles will then be applied to two examples which will demonstrate which insecurities could still arise in the pre-review in practice.

I. Einleitung

Als neues Instrument führte Art. 35 DS-GVO die Datenschutz-Folgenabschätzung (DSFA) ein, um die aus einer Datenverarbeitung folgenden Risiken für die Rechte und Freiheiten natürlicher Personen zu identifizieren, zu bewerten, kontinuierlich zu überwachen sowie ggf. durch geeignete Gegenmaßnahmen zu begrenzen.[1] Damit ist die DSFA ein zentrales Element des risikobasierten Ansatzes der DS-GVO. Dieser zielt darauf ab, die jeweiligen Pflichten des Verantwortlichen auf die Höhe des Risikos der Verarbeitung abzustimmen.[2]

Eine DSFA ist gem. Art. 35 Abs. 1 Satz 1 DS-GVO dann durchzuführen, wenn eine Datenverarbeitung voraussichtlich mit einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen verbunden ist. Damit stellt sich dem Verantwortlichen die Frage, ob hinsichtlich einer konkreten Datenverarbeitung eine DSFA erforderlich ist. Bislang nur ansatzweise wird die Frage diskutiert, wie eine solche, der eigentlichen DSFA vorgelagerte Vorprüfung konkret durchzuführen ist, um den Vorgaben der DS-GVO zu genügen.[3]

Nach einem Blick auf die frühere Rechtslage wird in diesem Beitrag diskutiert, nach welchen Maßstäben das Risiko einer Datenverarbeitung i.R.e. solchen Vorprüfung vom Verantwortlichen zu bewerten ist, um festzustellen, ob eine DSFA obligatorisch ist. Vergleichend wird hierzu die Leitlinie des *Europäischen Datenschutzausschusses (EDSA)*[4] herangezogen. Anhand von zwei

1 *Schmitz/von Dall'Armi*, ZD 2017, 57.
2 *Veil*, ZD 2015, 347, 348 und *Albrecht*, in: Simitis, Datenschutzrecht, 2019, Einl., Rdnr. 200.
3 S. z.B. *Bieker/Bremert/Hansen*, DuD 2018, 495; *DSK*, 2018, Kurzpapier Nr. 5, S. 1 f., abrufbar unter: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf; *Wichtermann*, DuD 2016, 798 f.
4 *Art. 29-Datenschutzgruppe*, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung i.S.d. VO 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt", WP 248 Rev. 01, 2017, vom *EDSA* am 25.5.2018 bestätigt, abrufbar unter: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

vermeintlich unproblematischen Beispielen werden die Schwierigkeiten demonstriert, die sich dennoch bei der Beurteilung des konkreten Einzelfalls i.R.d. Vorprüfung ergeben können.

II. Vergleich mit der früheren Rechtslage

1. Erforderlichkeit der Vorabkontrolle nach Art. 20 DS-RL

Gem. Art. 20 Abs. 1 RL 95/46/EG (DS-RL) oblag es den Mitgliedstaaten, festzulegen, welche Verarbeitungen so spezifische Risiken für die Rechte und Freiheiten der Personen beinhalten können, dass eine Vorabkontrolle durchzuführen war. Anhaltspunkte dafür, wann eine Verarbeitung mit „besonderen Risiken" einherging, konnten aus den beiden Regelbeispielen in § 4d Abs. 5 Satz 2 Nr. 1 und Nr. 2 BDSG a.F., der Verarbeitung besonderer Arten personenbezogener Daten und der Datenverarbeitung zum Zweck der Persönlichkeitsbewertung, abgeleitet werden.[5] Noch offener waren z.T. die Regelungen in den Landesdatenschutzgesetzen a.F., in Hessen z.B. musste der Verantwortliche gem. § 7 Abs. 6 Satz 1 HDSG a.F. vor dem Beginn jedes Verfahrens untersuchen, ob damit Gefahren für die geschützten Rechte der Betroffenen verbunden sind. In Deutschland oblag die Prüfung, ob eine Vorabkontrolle erforderlich war, gem. § 4d Abs. 5 BDSG a.F. dem Verantwortlichen.[6]

2. Erforderlichkeit der DSFA

Nach Art. 35 DS-GVO kommt den Mitgliedstaaten grundsätzlich keine Ausgestaltungsbefugnis mehr zu, wann eine DSFA durchzuführen ist. Nunmehr bestimmt Art. 35 Abs. 3 DS-GVO drei Fallgruppen, für die eine Pflicht zur Durchführung der DSFA besteht. Außerhalb dieser Regelbeispiele ist gem. Art. 35 Abs. 1 DS-GVO eine DSFA durchzuführen, wenn eine Form der Verarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Ausnahmen sind die von den nationalen Aufsichtsbehörden fakultativ zu erstellenden Listen nach Art. 35 Abs. 5 DS-GVO sowie Verarbeitungen auf Grundlage nationaler Erlaubnistatbestände nach Art. 35 Abs. 10 DS-GVO.

Der eigentlichen DSFA vorgelagert ist vom Verantwortlichen zu prüfen, ob die Verarbeitung unter eine Fallgruppe nach Art. 35 Abs. 3 DS-GVO subsumiert werden kann oder ob sie in der Liste der zuständigen Aufsichtsbehörde nach Art. 35 Abs. 4 DS-GVO enthalten ist oder ob sie nach Art. 35 Abs. 1 DS-GVO ein hohes Risiko zur Folge haben kann.[7] Es handelt sich daher abhängig von der Verarbeitung um ein mehrstufiges Prüfverfahren, das dem Verantwortlichen eine Bewertung des Risikos abverlangt.[8]

Zur Konkretisierung, wann eine DSFA erforderlich ist, hat die *Art. 29-Datenschutzgruppe* eine Leitlinie verabschiedet, die vom *EDSA* bestätigt wurde.[9] Ihr Ziel ist es, die Aufsichtsbehörden bei der Erstellung von Listen gem. Art. 35 Abs. 4 DS-GVO zu unterstützen. Die Leitlinie kann auch vom Verantwortlichen als Hilfestellung zur Risikobewertung herangezogen werden. Mittels neun Kriterien kann geprüft werden, ob für eine Verarbeitung ein hohes Risiko besteht und somit eine DSFA obligatorisch ist. Dies ist nach Auffassung des *EDSA* dann der Fall, wenn mindestens zwei Kriterien aus der Leitlinie zutreffend sind.[10] Als Kriterien werden genannt: das Bewerten und Einstufen, die automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung, die systematische Überwachung, die Verarbeitung vertraulicher Daten oder höchst persönlicher Daten, die Datenverarbeitung in großem Umfang, das Abgleichen oder Zusammenführen von Datensätzen, die Verarbeitung von Daten zu schutzbedürftigen Betroffenen, die innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen und Fälle, in denen die Verarbeitung an sich die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindert. Die Leitlinie ist nicht abschließend und beschreibt daher eine konkretere Menge an Verarbeitungsvorgängen, für die eine DSFA obligatorisch ist.[11]

III. Unter welchen Voraussetzungen ist eine DSFA durchzuführen?

Sofern sich nicht bereits aus Art. 35 Abs. 3 und Abs. 4 DS-GVO ergibt, dass eine DSFA durchzuführen ist, stellt sich aus Sicht der Praxis die Frage, wann von einem „hohen Risiko für die Rechte und Freiheiten natürlicher Personen" auszugehen ist, wann also die Vorprüfung zu dem Ergebnis führt, dass eine DSFA durchzuführen ist. Zur Konkretisierung des Begriffs des hohen Risikos führt Art. 35 Abs. 1 Satz 1 DS-GVO insbesondere auf den Einsatz von neuen Technologien sowie Art, Umfang, Umstände und Zweck der Verarbeitung hin, die in der DS-GVO nicht legaldefiniert sind.

1. Vorliegen eines „hohen Risikos"

Das Risiko bei der Verarbeitung von personenbezogenen Daten kann grundsätzlich „als Sachverhalt, in dem ein Schadenseintritt an einem Schutzgut möglich ist"[12], interpretiert werden. Im Rahmen dieser grundlegenden Systematisierung sind Risiken z.B. die Erhöhung individueller Verletzlichkeit, Diskriminierung oder Informationsemergenz.[13]

Im Rahmen der DS-GVO ist das Risiko für die Rechte und Freiheiten natürlicher Personen relevant.[14] Grundsätzlich gilt, dass sich ein Risiko aus der Schwere der Beeinträchtigung der Rechte und Freiheiten von natürlichen Personen (Eingriffsintensität), aus der sich die möglichen mittel- und unmittelbaren physischen, materiellen bzw. immateriellen Schäden und deren Ausmaß für die betroffenen Personen bestimmen lassen, und der Eintrittswahrscheinlichkeit ermitteln lässt.[15] Der Bezug zur Schwere des Schadens lässt sich mittels Erwägungsgrund 75 DS-GVO herstellen, in dem zumindest exemplarisch Schadensszenarien beschrieben werden (Risikokatalog).[16]

Wenn diese beiden Dimensionen auch i.R.d. Art. 35 Abs. 1 DS-GVO zu berücksichtigen wären, also sowohl die Eintrittswahrscheinlichkeit als auch die Schäden für die Betroffenen, so hätte dies allerdings zur Folge, dass bereits i.R.d. Vorprüfung, ob überhaupt eine DSFA durchzuführen ist, ein Großteil der DSFA vorweggenommen werden müsste.[17] Denn Eintrittswahrscheinlichkeiten lassen sich grundsätzlich erst bestimmen, wenn die Ereignisse, die zu einem Schaden führen können, und die getroffenen Abhilfemaßnahmen in Beziehung gesetzt sowie bewertet worden sind, d.h. wenn nach Art. 35 Abs. 7 DS-GVO, dem Kern der DSFA, vorgegangen wurde.[18] Z.B. erst durch die gezielte

---

5 *Meltzian*, in: BeckOK DatenschutzR, 23. Aufl. 2018, BDSG a.F. § 4d Rdnr. 34.
6 *Petri*, in: Simitis, Bundesdatenschutzgesetz, 8. Aufl. 2014, BDSG a.F. § 4d Rdnr. 33.
7 *Karg*, in: Simitis (o. Fußn. 2), Art. 35 Abs. 3 Rdnr. 36.
8 *Jandt*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, DS-GVO Art. 35 Abs. 1 Rdnr. 7.
9 *Art. 29-Datenschutzgruppe* (o. Fußn. 4), S. 5.
10 *Art. 29-Datenschutzgruppe* (o. Fußn. 4), S. 10-13.
11 *Art. 29-Datenschutzgruppe* (o. Fußn. 4), S. 10.
12 *Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 16.
13 *Drackert* (o. Fußn. 12), S. 291-306.
14 *Bieker*, DuD 2018, 29.
15 *Bieker* DuD 2018, 29, 30 f.; *Bieker/Bremert/Hansen*, DuD 2018, 493; *DSK*, 2018, Kurzpapier Nr. 18, S. 1, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf.
16 *Schmitz/von Dall'Armi*, ZD 2017, 57, 59.
17 So in der Tat z.B. *Karg* (o. Fußn. 7), Art. 35 Abs. 1 Rdnr. 22 f.
18 *Bieker/Hansen/Friedewald*, RDV 2016, 196; *Friedewald/Bieker/Obersteller* et al., White Paper Datenschutz-Folgenabschätzung – Ein Werkzeug für einen besseren Datenschutz, 3. Aufl. 2017, S. 32 f.

Auswahl und Prüfung von Abhilfemaßnahmen unter Berücksichtigung des Stands der Technik nach Art. 32 Abs. 1 DS-GVO, wie die Bewertung der Passwortstärke oder eine Multifaktor-Authentifizierung,[19] kann die Eintrittswahrscheinlichkeit für das Risiko in einem konkreten Verfahren bewertet werden. Die Folge in der Praxis wäre, dass die Prüfung, ob eine DSFA durchzuführen ist, und die eigentliche DSFA weitgehend übereinstimmen. Die Durchführung der DSFA würde somit faktisch zum Regelfall.

Dies kann nicht dem Ziel des Verordnungsgebers entsprechen, der – anders als andere Regelungen, die an ein Risiko anknüpfen (z.B. Art. 33 Abs. 1 DS-GVO) – eine DSFA explizit nur bei einem „hohen Risiko" voraussetzt. Zur Bewertung, ob mit einer Verarbeitung ein hohes Risiko einhergeht, bedarf es damit einer Prognose, ob ein bestimmter Risikograd überschritten wird. Die Vorprüfung zur DSFA ist deshalb eine Schwellwertanalyse, d.h. eine Abschätzung des Risikograds durch den Verantwortlichen.[20]

Unklar ist aber, wann von einem „hohen Risiko" in Abgrenzung zu einem „normalen" Risiko auszugehen ist. Diese Unterscheidung findet lediglich in Erwägungsgrund 76 DS-GVO eine kurze Erwähnung. Zur Abgrenzung wird das hohe Risiko in den Erwägungsgründen 89, 91 und 94 DS-GVO durch Beispiele untersetzt, z.B. wenn Verarbeitungsvorgänge den betroffenen Personen die Ausübung ihrer Rechte erschweren. Denkbar wäre es natürlich, ein hohes Risiko anzunehmen, wenn eine hohe Eintrittswahrscheinlichkeit für ein Ereignis besteht, das eine erwünschte oder eine unerwünschte Verarbeitung sein kann, und/oder wenn dieses Ereignis zu einem hohen Schaden für die Betroffenen führen kann. Allerdings würde diese Auslegung, die sowohl die Eingriffsintensität als auch die Eintrittswahrscheinlichkeit berücksichtigt, wie dargestellt dazu führen, dass faktisch ein Großteil der eigentlichen DSFA vorweggenommen würde. Unter Berücksichtigung des Zwecks der DSFA kann dies nicht der Intention des Gesetzgebers entsprechen, der die Einführung von stringenten Regeln in allen Mitgliedstaaten für sensible Verarbeitungen, d.h. mit hohem Risiko, erzielen wollte.[21]

Die Stellungnahmen des *EDSA* zu den vorgelegten Listen der Aufsichtsbehörden nach Art. 35 Abs. 4 DS-GVO lassen ebenfalls den Schluss zu, dass nicht in jedem Fall eine DSFA durchzuführen ist. So ziehen nach Auffassung des *EDSA* z.B. ein Joint Controllership bzw. die Verarbeitung von genetischen Daten nicht in jedem Fall eine DSFA nach sich, d.h. für ein hohes Risiko müssen weitere Kriterien vorliegen.[22]

Damit die Schwellwertanalyse ihrer Filterfunktion gerecht werden kann, spricht vieles dafür, dass zur Prüfung der Frage, ob eine Verarbeitung mit einem hohem Risiko einhergeht, ausschließlich das Kriterium herangezogen wird, ob mittels der Verarbeitung ein hoher Schaden für die Betroffenen möglich ist. Das Kriterium der Eintrittswahrscheinlichkeit sollte dagegen angesichts des damit verbundenen Prüfaufwands i.R.d. Vorprüfung, ob überhaupt eine DSFA durchzuführen ist, keine Berücksichtigung finden. Dies impliziert, dass der Risikobegriff i.S.d. Art. 35 Abs. 1 DS-GVO – abweichend von dem Risikobegriff im Kontext anderer Regelungen – i.R.d. Vorprüfung, ob eine DSFA durchzuführen ist, allein auf die möglichen Folgen, d.h. Schäden, ausgelegt wird. Dabei ist es für den Filter zunächst unerheblich, ob der Schaden durch eine erwünschte oder eine unerwünschte Verarbeitung, durch eine unzureichende Datensicherheit etc. hervorgerufen wird. Dies sowie die Eintrittswahrscheinlichkeiten, aber auch die Sicherheit der Verarbeitung nach Art. 32 DS-GVO werden erst i.R.d. eigentlichen DSFA untersucht und bewertet. Diese Vorgehensweise soll selbstverständlich nicht den risikobasierten Ansatz der DS-GVO entwerten, sondern zu ihrer sachgerechten Handhabung in der Praxis beitragen. Selbstverständlich gelten die Pflichten zur Gewährleistung der Sicherheit der Verarbeitung aus Art. 32 DS-GVO unabhängig von der hier vorgeschlagenen Auslegung, die allein dem Zweck dient, der Filterfunktion des Art. 35 Abs. 1 DS-GVO gerecht zu werden.

2. Auslegung der Indikatoren

Zur Bewertung des Risikos führt die DS-GVO Indikatoren ein: Art, Umfang, Umstände sowie Zwecke der Verarbeitung. Aus dem Gesetzestext geht nicht eindeutig hervor, ob hinsichtlich aller Indikatoren ein hohes Risiko gegeben sein muss oder ob eine DSFA bereits dann durchzuführen ist, wenn hinsichtlich eines Indikators, z.B. der Art von Verarbeitung, der Schwellwert für ein hohes Risiko überschritten wird.[23] Die Regelbeispiele des Art. 35 Abs. 3 DS-GVO sprechen dafür, dass bereits einzelne Indikatoren ein hohes Risiko begründen können.

Eine Analyse der Kommentarliteratur zeigt, dass die Indikatoren nicht einheitlich ausgelegt werden, insbesondere hinsichtlich der Art, der Umstände und des Umfangs der Verarbeitung. Unter Art der Verarbeitung werden die Datenarten, wie z.B. Gesundheitsdaten,[24] oder die Verarbeitung gem. Art. 4 Nr. 2 DS-GVO[25] verstanden. Unter den Umständen wird die konkrete Umsetzung der Datenverarbeitung verstanden[26] oder „alle tatsächlichen und rechtlichen Gegebenheiten, welche die Verarbeitung betreffen"[27]. Unter dem Umfang werden verschiedene Aspekte verstanden: die räumliche Verarbeitung (Stichwort: internationaler Datenverkehr), ggf. die Verteilung der Verantwortung auf mehrere Verantwortliche und die Menge der betroffenen Personen[28]. Unter Berücksichtigung der Gesetzessystematik und um eine praxisnahe Handhabung zu ermöglichen, spricht vieles dafür, die Indikatoren wie folgt auszulegen:

a) Art

Mit dem Indikator wird die inhaltliche, rechtliche und technische Ausgestaltung des Verarbeitungsvorgangs umfasst. Der Indikator bezieht sich somit auf alle wesentlichen Eigenschaften, die den Verarbeitungsvorgang kennzeichnen. Mit der Art der Verarbeitung wird die Planungsphase vor Beginn des Verarbeitungsvorgangs und i.S.e. kontinuierlichen Prozesses der regelmäßigen Prüfung des Verarbeitungsvorgangs auch der gesamte Lebenszyklus der Verarbeitung umfasst. Dies findet seinen Niederschlag in Art. 35 Abs. 11 DS-GVO.

b) Umfang

Der Indikator bezieht sich auf die Quantität und Qualität des Verarbeitungsvorgangs, d.h. insbesondere auch auf die Menge der Daten, die zu einer oder mehreren betroffenen Personen zugeordnet werden können. Die Qualität bezieht sich z.B. auf die Sensibilität der Daten.

c) Umstände

Der Indikator bezieht die konkreten Einzelheiten und speziellen Gegebenheiten ein, d.h. Kontextfaktoren, unter denen der Verarbeitungsvorgang in der Realität abgebildet wird. Der Gesetz-

19 *Bundesverband IT-Sicherheit e.V. (TeleTrusT)*, Handreichung zum „Stand der Technik", 2019, S. 18, 21.
20 *Bieker/Bremert/Hansen*, DuD 2018, 495; *DSK* (o. Fußn. 3), S. 1.
21 *EU-Kommission*, SEC(2012) 72 final, S. 58; *Rat der Europäischen Union*, 2014, 13772/14, S. 3 f., 27; *BayLDA*, Trilog-Synopse der DS-GVO, 2016, S. 248-254, abrufbar unter: https://www.lda.bayern.de/media/baylda_synopse.pdf.
22 *EDSA*, Opinion 01-27/2018 und 01-02/2019, abrufbar unter: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en.
23 *Jandt* (o. Fußn. 8).
24 *Piltz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 24 Rdnr. 33.
25 *Jandt* (o. Fußn. 8), Art. 32 Rdnr. 12 und *Martini*; in: Paal/Pauly, DS-GVO/BDSG, 2. Aufl. 2018, Art. 24 Rdnr. 32.
26 *Jandt* (o. Fußn. 8), Art. 32 Rdnr. 12.
27 *Piltz* (o. Fußn. 24), Art. 24 Rdnr. 35.
28 *Karg* (o. Fußn. 7), Art. 35 Abs. 1 Rdnr. 33.

geber adressiert über diesen Indikator die Umsetzung und Praxis des Verarbeitungsvorgangs. Dies kommt zum Ausdruck in der gleichen Systematik der Verwendung des Indikators in Art. 32 Abs. 1 DS-GVO, denn zu technischen Aspekten kann häufig erst in der Implementierung eine Aussage zum konkreten Risiko für die betroffene Person getroffen werden.

d) Zweck

Der Zweck der Verarbeitung ist die Beschreibung des Zustands, der durch das Mittel der Verarbeitung erreicht werden soll.[29]

e) Zusammenfassung

Die Indikatoren umfassen somit alle qualitativen und quantitativen Eigenschaften des Verarbeitungsvorgangs, anhand derer das Risiko für die betroffene Person objektiv und nachvollziehbar[30] i.R.d. Vorprüfung abgeschätzt werden kann. Welche konkreten Eigenschaften dies ermöglichen, muss im jeweiligen Einzelfall des Verarbeitungsvorgangs gesehen werden.

IV. Anwendung auf zwei Praxisbeispiele

Nachdem der Beitrag bislang versucht hat, die Maßstäbe für die Vorprüfung, ob im Einzelfall eine DSFA durchzuführen ist, zu konkretisieren, sollen die hierbei entwickelten Ansätze im Folgenden auf zwei für Hochschulen typische Praxisbeispiele, zum einen die Verarbeitung von Metadaten zum Zweck des Forschungsdatenmanagements und zum anderen die universitäre Stunden- und Raumplanung, angewendet werden. Es wurden bewusst Beispiele gewählt, bei denen prima facie davon auszugehen ist, dass sie in der Regel nicht mit einem hohen Risiko verknüpft sind. Es zeigt sich aber, dass auch bei vermeintlich unkritischen Verarbeitungssituationen weiterhin viele Rechtsunsicherheiten bestehen bleiben.

1. Verarbeitung von Metadaten zum Zweck des Forschungsdatenmanagements

Die Verarbeitung dient dem Zweck der Langfristaufbewahrung von Forschungsdaten. So empfiehlt die *Deutsche Forschungsgemeinschaft (DFG)* eine Aufbewahrung von zehn Jahren für Primärdaten.[31] Hierbei geht es um die Nachvollziehbarkeit und Nachnutzung von wissenschaftlichen Ergebnissen. Unter Primärdaten sind die Daten der einzelnen Arbeitsschritte zu verstehen, die i.E. zu einem wissenschaftlichen Ergebnis geführt haben, wie z.B. Messergebnisse, Studienerhebungen oder personenbezogene Daten von Probanden.

Primärdaten sollten grundsätzlich mit Informationen über die Wissenschaftler verknüpft sein, die für die Publikation verantwortlich sind. Die jeweils anzugebenden Metadaten sind durch das verwendete Metadatenschema vorgegeben. Hierbei handelt es sich z.B. um den Namen und die Affiliation des zugehörigen Wissenschaftlers. Durch die Verknüpfung der Meta- mit den Primärdaten wird der Aussagegehalt zu einer Person jedoch maßgeblich beeinflusst. Je mehr Primärdaten über die Metadaten einer Person zugeordnet sind, umso größer wird dadurch der Umfang der Verarbeitung. Wenn sich aus den Metadaten z.B. ergibt, zu welchem Zeitpunkt die jeweiligen Primärdaten erhoben wurden, dann könnte dies die Analysierbarkeit des Arbeitsverhaltens von Beschäftigten anhand der Metadaten, z.B. anhand von Arbeitszeiten, ermöglichen. Soweit die Primär- und die Metadaten öffentlich zugänglich gemacht werden, wirft dies außerdem die Frage auf, inwieweit in der Praxis eine Risikoabschätzung durch den Verantwortlichen möglich ist, wenn personenbezogene Daten offengelegt werden.[32]

Bei Auswertung der Indikatoren des Art. 35 Abs. 1 DS-GVO und einer wertenden Betrachtung ist trotz dieser Unwägbarkeiten grundsätzlich davon auszugehen, dass derartige Formen der Verarbeitung nicht mit einem hohen Risiko verbunden sind, sofern keine Besonderheiten im Einzelfall vorliegen, da die Daten in der Regel mit dem Einverständnis des betroffenen Wissenschaftlers verarbeitet werden. Wissenschaftlerinnen und Wissenschaftler haben darüber hinaus grundsätzlich ein Eigeninteresse an der Publikation ihrer Daten. Einige Daten, z.B. die jeweilige Affiliation, werden in der Regel ohnehin öffentlich zugänglich sein. Die Ausblendung der Eintrittswahrscheinlichkeit in der Vorprüfung ist für diese Formen der Verarbeitung sachgerecht, da die möglichen Schäden für die Wissenschaftler als gering abgeschätzt werden können und somit die Eintrittswahrscheinlichkeit das Risiko nicht signifikant erhöhen würde. Eine DSFA wird daher in der Regel nicht erforderlich sein.

Ein Abgleich mit den Kriterien aus der Leitlinie des *EDSA*[33] zeigt allerdings, dass durchaus zwei oder mehr Kriterien erfüllt sein können: Die Metadaten können grundsätzlich dazu geeignet sein, Profile über Wissenschaftlerinnen und Wissenschaftler zu erstellen, auch wenn dies nicht der primäre Zweck der Verarbeitung ist (Kriterium: „Bewerten und Einstufen"). Weiterhin kann über die Menge der Metadaten und deren Verknüpfung zu Primärdaten das Kriterium „Datenverarbeitung im großen Umfang" zutreffend sein. Beim Forschungsdatenmanagement werden zudem in der Regel innovative technische Lösungen eingesetzt. Bei strikter Anwendung der Leitlinie des *EDSA* würde man daher den Schluss ziehen müssen, dass eine DSFA obligatorisch ist, weil mindestens zwei Kriterien zutreffend sind. Dies zeigt, dass auch die Leitlinie des *EDSA* einer Auslegung bedarf und die Schwere des Schadens hierbei einbezogen werden sollte.

2. Universitäre Stunden- und Raumplanung

Ein komplexer Teilprozess an Universitäten ist die Stunden- und Raumplanung zur Organisation sowie Durchführung von Lehrveranstaltungen. Anforderungen von Lehrenden zu Raumeigenschaften und zum Zeitmanagement müssen Berücksichtigung finden, um eine optimale Ressourcen- sowie Stundenplanung und somit einen reibungslosen Lehrbetrieb sicherstellen zu können.

Mit diesem administrativen Vorgang wird zwar grundsätzlich kein hohes Risiko verbunden sein, z.T. wird nicht einmal die Verarbeitung personenbezogener Daten erforderlich werden. Dies kann jedoch je nach der Art der Verarbeitung und deren Zweckbestimmung variieren. Vorstellbar ist, dass zur Stunden- und Raumplanung auch Angaben zu Behinderungen und zur Barrierefreiheit verarbeitet werden müssen, die als sensible Daten i.S.v. Art. 9 DS-GVO einzuordnen sind, und dadurch eine andere Abschätzung des Risikos notwendig wird. Dies ist auch der Fall, wenn weitere Verfahren betrachtet werden müssen, die i.R.e. integrierten Studierendenmanagements eine erhebliche Auswirkung für die Betroffenen haben können, wie z.B. die komplette elektronische Abwicklung von Prüfungen (E-Assessments).[34]

Zu berücksichtigen ist auch, ob die betrachtete Verarbeitung sich als Teil in eine größere Verarbeitung einbettet und somit durch eine mögliche Zusammenführung von Daten zwangsläufig eine andere Risikoabschätzung bedingt. Daraus ergibt sich die Frage, mit welcher Granularität ein Verfahren bzw. eine Form der Verarbeitung grundsätzlich zu definieren ist, um eine

---

29 *Roßnagel*, in: Simitis (o. Fußn. 2), Art. 5 Abs. 1 lit. b Rdnr. 68.
30 *Nolte/Werkmeister*, in: Gola (o. Fußn. 24), Art. 35 Rdnr. 1.
31 *Deutsche Forschungsgemeinschaft (DFG)*, Sicherung guter wissenschaftlicher Praxis/Safeguarding Good Scientific Practice, ergänzte Aufl. 2013, S. 21 f.
32 S. dazu allg. *Roßnagel* (o. Fußn. 29), Art. 4 Nr. 2 Rdnr. 25 f.
33 *Art. 29-Datenschutzgruppe* (o. Fußn. 4), S. 10-13.
34 *Forgó/Graup/Pfeiffenbring*, Gutachten über rechtliche Aspekte von E-Assessments an Hochschulen, 2016, S. 45.

Vorprüfung durchführen zu können. Eine ungenügende Granularität kann zu einem falschen Ergebnis der Prüfung führen.

V. Fazit und Ausblick

Es muss konstatiert werden, dass eine rechtssichere Vorprüfung, ob eine Form der Verarbeitung ein hohes Risiko aufweist und somit eine DSFA erforderlich ist, für den Verantwortlichen derzeit problematisch ist. Durch die Unschärfe des Regelungsinstrumentariums besteht außerdem die Gefahr von Dysfunktionalitäten, z.B. durch eine mögliche Überregulierung bei Verarbeitungen, für die offensichtlich kein hohes Risiko angenommen werden muss,[35] wie anhand des Beispiels Forschungsdatenmanagement gezeigt. Die risikobasierte Pflichtenausprägung droht auf Grund der vorliegenden Unbestimmtheit im Grundsatz zu scheitern,[36] zumindest was die DSFA betrifft. Dies wiegt besonders schwer, weil die DSFA ein wesentliches Instrumentarium sein soll, um die möglichen Schäden für die Betroffenen bei risikobehafteten Verarbeitungen zu minimieren.

Um hier gegenzusteuern, sind nunmehr insbesondere die Aufsichtsbehörden und der *EDSA* gefordert. Darüber hinaus kann über die Erarbeitung von Verhaltensregeln nach Art. 40 DS-GVO durch Verbände bzw. Vereinigungen eine Konkretisierung erreicht werden.

Für die Praxis kann es, wie anhand der Beispiele gezeigt, zunächst sachgerecht sein, den Risikobegriff nach Art. 35 Abs. 1 DS-GVO als Filter für die DSFA so auszulegen, dass ausschließlich die Abschätzung der Schwere der möglichen Schäden für die Betroffenen herangezogen wird. Die vorgestellte Auslegung der Indikatoren kann hierfür eine erste Grundlage zur weiteren Ausgestaltung der Vorprüfung sein.

Jens Syckor
ist IT-Sicherheitsbeauftragter an der TU Dresden.

Prof. Dr. Thorsten Strufe
ist Inhaber des Lehrstuhls für Datenschutz und Datensicherheit an der TU Dresden.

Prof. Dr. Anne Lauber-Rönsberg
ist Juniorprofessorin für Bürgerliches Recht, Immaterialgüterrecht sowie Medien- und Datenschutzrecht an der TU Dresden.

35 *von Lewinski*, Die Matrix des Datenschutzes, 2014, S. 83-85.
36 *Roßnagel*, DuD 2016, 564 f.